UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

UNITED STATES OF AMERICA	)	
	)	
v.	)	**Criminal No. 1:16-CR-00053**
	)	
HAMZA KOLSUZ,	)	
	)	**Trial: May 16, 2016**
Defendant.	)	

DEFENDANT HAMZA KOLSUZ'S MOTION TO SUPPRESS EVIDENCE

Comes now, Defendant HAMZA KOLSUZ, by counsel, and respectfully submits this Motion to Suppress Evidence.

INTRODUCTION

Mr. Kolsuz is a citizen of Turkey and visited the United States pursuant to a tourist visa between January 25, 2016, and February 3, 2016. On February 3, 2016, Customs and Border Patrol agents allegedly found various handgun parts in Mr. Kolsuz's checked luggage for an outbound return flight to Istanbul, Turkey. Mr. Kolsuz was arrested. After Mr. Kolsuz's arrest, without a warrant and without Mr. Kolsuz's consent, law enforcement officers conducted a seizure and forensic search of his cell phone that lasted from the arrest through March 3, 2016.

None of the exceptions to the Fourth Amendment's warrant requirement apply in this case. Specifically, the Fourth Amendment does not permit warrantless searches of cell phones incident to arrest. *Riley v. California*, 134 S.Ct. 2473 (2014). Moreover, the border search exception for warrantless searches is inapplicable because the governmental interests that justify border searches were not at stake here. Agents seized Mr. Kolsuz's phone and commenced its forensic search after it was already determined that the phone would not cross the border. To find that this search was justified here "would mean that the border search doctrine has no borders." *See United States v. Kim*, 103 F. Supp. 3d 32, 35 (D.D.C. 2015). Accordingly, Mr. Kolsuz moves to suppress any evidence contained within or otherwise obtained from, or as the fruit of, the unconstitutional search of his cell phone.

BACKGROUND

Mr. Kolsuz is charged in a three-count indictment with attempting to violate the Arms Export Control Act, 22 U.S.C. 2778, attempting to smuggle goods from the United States in violation of 18 U.S.C. § 554, and conspiracy to commit those offenses in violation of 18 U.S.C. § 371.

On the evening of February 2, 2016, Mr. Kolsuz boarded a plane in Cleveland, Ohio, and his ultimate destination was Istanbul, Turkey, with a stop at Dulles International Airport. According to the allegations in the indictment, on the morning of February 3, 2016, a customs inspection performed by Customs and Border Patrol officers at Dulles International Airport revealed an assortment of handgun parts contained in Mr. Kolsuz's checked luggage. Mr. Kolsuz was arrested on February 3, 2016, and has remained in federal custody since this time. While none of the handgun parts constituted an actual firearm, or required a person to have a license to possess them, or were illegal to transport in one's luggage, the Arms Export Control Act ("AECA") (22 U.S.C. § 2778) prohibits the exportation without a license of "military aircraft, helicopters, artillery, shells, missiles, rockets, bombs, vessels of war, explosives, military and space electronics, and certain firearms." USSG § 2M5.2, Application Note 1. The AECA also prohibits the unlicensed export of handgun parts.

According to discovery provided thus far by the government, following the arrest of Mr. Kolsuz, Homeland Security Special Agent ("SA") Adam Coppolo transported, among other things, Mr. Kolsuz's mobile phone to the Homeland Security office located in Sterling, Virginia.

SA Coppolo then requested the assistance of Computer Forensic Agent ("CFA") Michael Del Vacchio in extracting information from Mr. Kolsuz's phone (which was an iPhone, and thus could more aptly be described as a computer than a phone because such devices collect and store vast quantities of digital information unrelated to telephonic communication). This report was used by SA Coppolo to conduct a "border search" of the iPhone. According to the law enforcement report of the search, the purpose of the search of the phone was to find evidence relating to the charge on which Mr. Kolsuz had been arrested. This purported border search, which occurred at an office building in Sterling, Virginia, commenced after Mr. Kolsuz had been arrested and lasted for a full month, concluding on or about March 3, 2016. At no time during this search was the phone in the process of crossing the border, about to cross the border, or in danger of crossing the border.

The forensic report that resulted from the iPhone search is 896 pages in length. It details Mr. Kolsuz's internet browsing history, text messages, emails, previous GPS locations down to exact addresses, and calendar appointments dating years into the future.

ARGUMENT

Warrantless searches of cell phones seized from arrested persons are no longer justified by the "search incident to arrest" exception to the Fourth Amendment's warrant requirement. *Riley v. California*, 134 S.Ct. 2473 (2014). The government, however, attempts to justify the search in this case under the "border search" exception, which generally allows for "exhaustive forensic searches" of electronic devices at the border upon reasonable suspicion. *United States v. Cotterman*, 709 F.3d 952 (9th Cir. 2013). The issue is whether, after *Riley*, the "border search" exception may be extended to the search of an arrestee's cell phone seized incident to an arrest at the border, when the arrestee is no longer in the process of crossing the border or attempting to cross the border. In other words, while law enforcement may delay a person crossing the border to perform an exhaustive forensic search of his electronic devices before he leaves the country, may law enforcement arrest a person and seize his electronic device, thus removing any possibility of it crossing the border, and still rely on the border-search exception to conduct a subsequent search of the device for evidence of the crime for which the person has been arrested?

A. After *Riley*, the Border Search Exception Does Not Extend to the Search of Mr. Kolsuz's Cell Phone Pursuant to His Arrest.

1. The Exceptions to the Warrant Requirement are Narrowly Construed

The ultimate touchstone of the Fourth Amendment is reasonableness. *Riley*, 134 S.Ct. at 2482. "Where a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing … reasonableness generally requires the obtaining of a judicial warrant." *Id.* In the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement. *Id.* Because warrantless searches and seizures are *per se* unreasonable, the government bears the burden of showing that a warrantless search or seizure falls within an exception to the Fourth Amendment's warrant requirement. *United States v. Cervantes*, 703 F.3d 1135, 1141 (9th Cir. 2012). Exceptions to the Fourth Amendment's warrant requirement must be "jealously and carefully drawn," accompanied by "a showing by those who seek exemption that the exigencies of the situation made that course imperative." *Coolidge v. New Hampshire*, 403 U.S. 443, 455 (1971) (internal quotations and citations omitted). Indeed, the Supreme Court has recently emphasized that warrant exceptions are narrowly construed in light of their original justification. *See Arizona v. Gant*, 556 U.S. 332 (2009). Specifically, the Court held that a warrantless search violated the Fourth Amendment where an exception to the warrant requirement was asserted in a manner unjustified by the original basis for the exception.

Id. at 343 (warrant exception cannot apply in circumstances where its application would "untether the rule from the justifications underlying" the exception).

In *Riley*, the Supreme Court held that "the search incident to arrest exception does not apply to cell phones," and thus, that "a warrant is generally required . . . even when a cell phone is seized incident to arrest." 134 S.Ct. at 2493-94. Generally, the "search incident" doctrine allows police to "discover and seize the fruits or evidences of crime" for reasons of evidence preservation or officer safety. *Id.* at 2482-84. However, in balancing the competing interests of privacy and law enforcement needs in the context of cell phone searches incident to arrest, the Court concluded that "[m]odern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse," *id.* at 2488-89, and that "a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house." *Id.* at 2491 (emphasis in original). *Riley* noted that "other case-specific exceptions may still justify a warrantless search of a particular phone," and it discussed the exigency exception, but it made no mention of the "border search" exception. *Id.* at 2494.

2. The Border Search Exception Does Not Apply When the Search is Conducted to Find Evidence Not Contraband At the Border

Under the "border search" exception, the government may conduct "routine" searches of persons and effects at the border or its functional equivalent upon no suspicion, *United States v. Flores-Montano*, 541 U.S. 149, 152 (2004), and "nonroutine" searches—i.e., highly intrusive searches—upon reasonable suspicion. *United States v. Montoya de Hernandez*, 473 U.S. 531 (1985). However, the scope and reach of the "border search" exception is determined by reference to its historical scope and rationale. *United States v. Ramsey*, 431 U.S. 606, 620-622 (1977) (examining "the rationale behind the border-search exception" and "historically recognized scope of the border-search doctrine" to uphold a suspicionless search of mail at the border). In this regard, "searches made at the border, pursuant to the longstanding right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border. *United States v. Ramsey*, 431 U.S. 606, 616, (1977).

Congress, since the beginning of our Government, "has granted the Executive plenary authority to conduct routine searches and seizures at the border, without probable cause or a warrant, in order to regulate the collection of duties and to prevent the introduction of contraband into this country." *United States v. Flores-Montano*, 541 U.S. 149, 152-53 (2004) (discussing plenary authority to protect territorial integrity to prevent "the entry of unwanted persons and effects") (citing *United States v. Montoya de Hernandez*, 473 U.S. at 537).

While the border search exception has been held to apply to searches both upon entry and exit, the underlying rationale rests on "fundamental principles of national sovereignty" and the "long-standing right of the sovereign to protect itself." *United States v. Oriakhi*, 57 F.3d 1290, 1296-97 (4th Cir. 1995) (holding that the sovereign has interest in regulating foreign commerce and controlling its currency). Importantly, the Supreme Court has justified warrantless border searches precisely because they are based on purposes *other than* furnishing evidence against a person. *Ramsey*, 431 U.S. at 616 (differentiating the "long-standing right of the sovereign to protect itself" and the "plenary customs power" from "the more limited power to enter and search" places or objects, which generally requires a warrant).

The "border search" exception is a narrow one and may not be extended beyond its historical purposes to a post-arrest, investigatory search of a cell phone seized incident to an arrest at the border. Here, Mr. Kolsuz was already arrested when the agents searched his phone. Additionally, both the phone and the allegedly illegal contraband—the gun parts detected by border patrol agents—had already been seized when the Homeland Security agents began to search his phone. At the time of the search of Mr. Kolsuz's phone, which lasted over a month, the government was not exercising its sovereign authority to monitor items entering or exiting the country, regulating commerce, controlling currency, or collecting any duties. Rather, the government's own report of the search concedes that it began to search the phone, after determining that it would not cross the border, for the purpose of gathering evidence relating to the charge upon which Mr. Kolsuz had been arrested.

In *United States v. Cotterman*, decided before the Supreme Court's opinion in *Riley*, the Ninth Circuit held that the government could take a laptop seized during a border search with reasonable suspicion and take it to another location to be forensically examined. However, there, the suspected contraband was the digital data itself (child pornography on the laptop). 709 F.3d 952, 958-59 (9th Cir. 2013). Moreover, the government seized the laptop upon the defendant's entry into the United States (while allowing the defendant and his wife to enter), and did not discover evidence of crime until later conducting the forensic search. *Id.* at 957-59. In other words, the search in *Cotterman* was conducted in furtherance of determining whether the laptop could be permitted to legally enter the United States.

Here, in contrast, at the time of the forensic search, the gun parts had already been seized, Mr. Kolsuz had already been arrested, and his cell phone had already been held as potential evidence. The cell phone itself was not contraband or a dutiable article. Nor was it, like the laptop in *Cotterman*, still in the process of crossing the border conditioned upon a search for contraband. As noted, the phone was not being searched to determine whether it could legally cross the border, but for evidence to be used in a criminal prosecution. Upon Mr. Kolsuz's arrest the agents were entitled to continue searching his personal effects because other exceptions applied to those items (i.e., search incident to arrest, inventory search, and inevitable discovery). A search of his cell phone for evidence of the crime for which he had been arrested, however, required a warrant. *See United States v. Camou*, 773 F.3d 932, 937-45 (9th Cir. 2014) (rejecting the government's attempt to justify a cell phone search at an interior border patrol checkpoint under the exigency, vehicle, good faith, search incident, and inevitable discovery exceptions).

Moreover, other courts considering the intersection of technology, the Fourth Amendment, and the border search exception, have held that the border search exception does not allow for warrantless searches of computer devices. In *United States v. Kim*, Judge Amy Berman Jackson concluded that the warrantless search of a traveler's laptop as he was departing the United States was unreasonable. In that case, DHS border patrol agents seized Mr. Kim's computer, cloned the hard drive, and sent it to a forensic lab roughly 150 miles from the airport. The Court stated that "there was little about this search—neither its location nor its scope and duration—that resembled a routine search at the border." *United States v. Kim*, 103 F. Supp. 3d 32, 35 (D.D.C. 2015). The Court accordingly held that the search was unreasonable and violated the Fourth Amendment. *Id*.

The search of Mr. Kolsuz's phone simply was not made during a border search. It was, instead, a search incident to his arrest and a warrant was therefore required. *See Riley v. California*, 134 S.Ct. 2473 (2014). In addition to the fact that the government had no sovereign border protection interests at stake here, a border search is one that occurs, by definition, at the border (or its functional equivalent, such as an airport). *See Almeida-Sanchez v. United States*, 413 U.S. 266, 272-73 (1973) (border searches "take place not only at the border itself, but at its functional equivalents as well"). Mr. Kolsuz's phone was not searched at the functional equivalent of the border. It does not appear that any customs agents even tried to gain access to the phone at the airport. Rather, the phone was not searched until it entered a secure Homeland Security facility located in an office building in Sterling, Virginia, roughly five miles away from the airport. Moreover, the search was not reasonably close in time to any attempted border crossing, as the search lasted for an entire month after Mr. Kolsuz's attempt to leave.

Furthermore, the search cannot be analyzed under the extended border search doctrine, as this doctrine justifies border searches done away from the physical border only where agents have reasonable suspicion "not only with respect to the nature of the material seized *but to the fact that it has indeed illegally crossed a border within a reasonably recent time*." *United States v. Bilir*, 592 F.2d 735, 739-740 (4th Cir. Md. 1979). This doctrine is inapposite to the search done here. Mr. Kolsuz's cell phone had not illegally crossed a border recently. In fact, it remains detained within the United States where it had been for the days preceding Mr. Kolsuz's arrest.

The government has acknowledged that the search was conducted to gather evidence to be used against Mr. Kolsuz in this proceeding—not in furtherance of any sovereign interest relating to securing the border, because it had already arrested Mr. Kolsuz and determined that neither he nor his phone would cross the border, at least until the conclusion of this criminal prosecution (at which time, of course, they would be subject to a border search before leaving).

B. The Government Could Have Easily Obtained a Warrant But Chose Not To Do So Here.

In the modern era of electronic communication, search warrants are easy to obtain, and do not even require an in-person application. *Missouri v. McNeely*, 133 S.Ct. 1552, 1561-62 (2013). The government is still in possession of Mr. Kolsuz's phone. If the government had a legal basis to search Mr. Kolsuz's cell phone, SA Copollo could easily have applied for and obtained a warrant for its search. The government chose, however, to forgo judicial authorization of its exhaustive forensic analysis of Mr. Kolsuz's smart phone. Instead, it conducted an intrusive, month-long forensic search for evidence to be used in this criminal prosecution, the reasons for which were entirely unrelated to the justifications supporting the border-search exception to the warrant requirement. In other words, it was not a border search, but a search incident to arrest. And it was conducted without a warrant in contravention of clear Supreme Court precedent on cell phone searches incident to arrest.

CONCLUSION

For the foregoing reasons, the Court should order the exclusion of all evidence derived from the warrantless search of Mr. Kolsuz's cell phone, and all evidence that was a fruit of that warrantless search.

Respectfully submitted,

HAMZA KOLSUZ

By Counsel,

Geremy Kamens,

Federal Public Defender

By: /s/

Todd Richman
Assistant Federal Public Defender
VA Bar Number 41834
Erica L. Marshall
Volunteer Attorney
VA Bar Number 78781
Attorneys for Hamza Kolsuz
Office of the Federal Public Defender
1650 King Street, Suite 500
Alexandria, Virginia 22314
703-600-0825
703-600-0880 (fax)
todd_richman@fd.org
erica_marshall@fd.org

CERTIFICATE OF SERVICE

I hereby certify that on March 30, 2016, I will electronically file the foregoing pleading with the Clerk of the Court using the CM/ECF system, which will then send a notification of such filing (NEF) to the following:

Heather Alpino
US Attorney's Office
2100 Jamieson Avenue
Alexandria, VA 22314
703-299-3700
Heather.alpino2@usdoj.gov

By: /s/

Erica L. Marshall
Volunteer Attorney
VA Bar Number 78781
Attorney for Hamza Kolsuz
Office of the Federal Public Defender
1650 King Street, Suite 500
Alexandria, Virginia 22314
703-600-0859
703-600-0880 (fax)
Erica_Marshall@fd.org